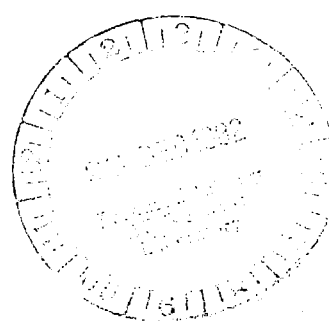
NASA Contractor Report 3566

CARE III Phase II Report - Mathematical Description

J. J. Stiffler and L. A. Bryant

CONTRACT NAS1-15072
NOVEMBER 1982

NASA



NASA Contractor Report 3566

CARE III Phase II Report - Mathematical Description

J. J. Stiffler and L. A. Bryant
Raytheon Company
Sudbury, Massachusetts

Prepared for
NASA Langley Research Center
and Air Force Avionics Laboratory
Wright-Patterson Air Force Base
under Contract NAS1-15072

National Aeronautics
and Space Administration

**Scientific and Technical
Information Branch**

1982

TABLE OF CONTENTS

List of Figures

List of Tables

LIST OF SYMBOLS

Symbol	Definition
$A(t\|\underline{\ell})$	See Table 1.
$A'(t\|\underline{\ell})$	See Table 1.
$a_x(t)$	See Table 1.
$a_{x_i}(t)$	See Table 1.
$a'(t\|\underline{\ell})$	See Table 1.
$B_{x_i,y_j}(t\|\underline{\ell})$	See Table 1.
$b_{x,y}(\nu_x,\nu_y)$	Probability that a stage-x fault and a stage-y fault form a critical pair given ν_x known stage-x faults and ν_y known stage-y faults.
C	Probability that a propagated error is detected before it causes the system to malfunction.
$C_{y_j}(t\|\underline{\ell})$	See Table 1.
$D_{x_i,y}(t\|\underline{\ell})$	See Table 1.
$d_{x_i}(t)$	Probability that a category-x_i error has not been detected t time units after its generation.
$e_{x_i}(t)$	Probability that a category-x_i error has not yet propagated t time units after its generation.
$H_X(t\|x_i)$ $X = L,\overline{B},B$	See Table 1.
$h_X(t\|x_i)$ $X = DPT,F$	See Table 1.
$h_{DF}(t\|x_i,y_j)$	See Table 1.

Symbol	Definition
$\underline{\ell}$	A vector, the components of which indicate the number of faulty elements in each stage ($\underline{\ell} = \ldots \ell_x, \ell_y, \ldots$).
$\underline{\ell} - \varepsilon_y$	$(\ldots \ell_x, \ell_y - 1, \ell_z, \ldots)$
ℓ_x	Number of stage-x modules that have experienced some fault ($\ell_x = \sum_i \ell_{x_i}$)
ℓ_{x_i}	Number of stage-x modules that have experienced category-x_i faults.
m_x	Minimum number of units needed for stage x to be operational.
n_x	Number of functional stage-x units available at time t = 0.
$P_{\underline{\ell}}$	State of operational system after exactly $\underline{\ell}$ failures.
$P(t)$	Element survival probability.
$P'(t)$	Rate of change of $P(t)$.
$P_{\underline{\ell}}(t)$	Probability that a system has sustained exactly $\underline{\ell}$ failures and is still operational at time t.
$P_{\underline{\ell}}^*(t)$	Probability that a system has sustained exactly $\underline{\ell}$ failures by time t.
$P(\mu_x, t \mid \ell_x)$	See Table 1.
P_A	Probability that a fault detected in the active state is diagnosed as permanent.
P_B	Probability that a fault detected in the benign state is diagnosed as permanent.
Q_ℓ	State of system that has failed after exactly $\underline{\ell}$ element failures.

Symbol	Definition
$Q_{\underline{\ell}}(t)$	Probability that a system has sustained exactly $\underline{\ell}$ failures and then malfunctioned by time t.
$r_{x_i}(t)$	Probability that a category-x_i fault has not resulted in an error t time units after it has become active.
$R(t)$	Reliability; probability that the system is operational at time t.
$r_{ij}(t)$	Transition rate between states S_i and S_j.
$R_x(t)$	See Table 1.
$R_{x_i}(t)$	See Table 1.
S_i	State i in a Markov chain.
$S_i(t)$	State i occupancy probability at time t.
$S_i'(t)$	Rate of change of $S_i(t)$.
x	Stage index.
α_{x_i}	Rate of transition from active to benign fault states.
β_{x_i}	Rate of transition from benign to active fault states.
$\delta_{x_i}(t)/d_{x_i}(t)$	Rate of detection of type-x_i faults t time units after they become active.
$\varepsilon_{x_i}(t)/e_{x_i}(t)$	Rate at which an error caused by a type-x_i fault is propagated following its generation at time t = 0.

Symbol	Definition
$\Lambda_{\underline{\ell}}(t,\tau)$	$\int_{\tau}^{t} \lambda_{\underline{\ell}}(\eta)\,d\eta$
$\lambda^{(1)}_{\underline{j\ell}}(t)$	Rate of occurrence of failures that take the system from state $P_{\underline{j}}$ to state $P_{\underline{\ell}}$.
$\lambda^{(2)}_{\underline{j\ell}}(t)$	Rate of occurrence of failures that take the system from state $P_{\underline{j}}$ to $Q_{\underline{\ell}}$.
$\lambda_{\underline{j\ell}}{}^{*}(t)$	$\lambda^{(1)}_{\underline{j\ell}}(t) + \lambda^{(2)}_{\underline{j\ell}}(t)$
$\lambda_{\underline{\ell}}(t)$	Transition rate out of state P_{ℓ}.
$\lambda_{\ell}{}^{*}(t)$	$\sum_{\underline{j} \neq \underline{\ell}} \lambda_{\ell j}{}^{*}(t)$
$\lambda_{x_i}(t)$	Rate of occurrence of category-x_i faults ($\lambda_{x_i}(t) = \omega_{x_i} \lambda_{x_i} t^{\omega_{x_i}-1}$).
$\underline{\mu}$	A vector, the components of which indicate the current number of latent faults in each stage ($\underline{\mu} = \ldots \mu_x, \mu_y, \ldots,$).
$\rho_{x_i}(t)/r_{x_i}(t)$	Error generation rate of a type-x_i fault t time units after it becomes active.
$\mu_{\underline{\ell}}(t)$	Transition rate from system state P_{ℓ} to system state Q_{ℓ} ($\mu_{\underline{\ell}}(t) = \mu^{(1)}_{\underline{\ell}}(t) + \mu^{(2)}_{\underline{\ell}}(t)$).
$\mu^{(1)}_{\ell}(t)$	Transition rate from state P_{ℓ} to state Q_{ℓ} due to single-fault coverage failures.
$\mu^{(2)}_{\ell}(t)$	Transition rate from state P_{ℓ} to state Q_{ℓ} due to double-fault coverage failures.

1. Introduction

CARE III (Computer-Aided Reliability Estimation, version three) is a computer program designed to help estimate the reliability of complex, redundant systems. Although the program can model a wide variety of redundant structures, it was developed specifically for fault-tolerant avionics systems - systems distinguished by the need for extremely reliable performance since a system failure could well result in the loss of human life.

It is usually relatively easy to design enough redundancy into a system to reduce to acceptably small levels the probability that it fails due to inadequate resources. The dominant cause of failure in ultra-reliable systems thus tends to be due not to the exhaustion of resources but rather to the failure to detect and isolate a malfunctioning element before it has caused the system to take an erroneous action. Such failures are called coverage failures. CARE III differs from its predecessors in, among other things, the attention given to coverage failure mechanisms.

The first CARE program, developed at the Jet Propulsion Laboratory in 1971, provided an aid for estimating the reliability of systems consisting of a combination of any of several standard configurations (e.g. standby-replacement configurations, triple-modular redundant configurations, etc.). CARE II was subsequently developed by Raytheon, under contract to the NASA Langley Research Center, in 1974. It substantially generalized the class of redundant configurations that could be accommodated, and included a coverage model to determine the various coverage probabilities as a function of the applicable fault recovery mechanisms (detection delay, diagnostic scheduling interval, isolation and recovery delay, etc.).

CARE III further generalizes the class of system structures that can be modeled and greatly expands the coverage model to take into account such effects as intermittent and transient faults, latent faults, error propagation, etc. In order to accomplish this, it was necessary to depart substantially from the approaches taken in previous reliability modeling efforts. The nature of, and the reasons for, this departure are explained in the following section.

2. Background

Reliability models tend to fall into one of two classes: combinatorial or Markov. Combinatorial models attempt to categorize the set of operational states (or, conversely, the number of non-operational states) of the system in terms of the functional states of its components in such a way that the probabilities of each of these states can be determined by combinatorial means. Markov models concentrate on the rate at which transitions take place between different system states and then use this information to determine the probabilities that the system is in each of these states at any given time. These two approaches, and the CARE III departure, are best illustrated by an example.

Consider a simple, redundant structure consisting of four identical elements, the (binary) outputs of which are passed through a majority voter. If the outputs of at least three of these units are correct, the voter output is likewise correct. Further, if any one unit is determined to be faulty, its outputs are subsequently ignored by the voter, so that a second failure can also be tolerated without producing an incorrect output. First, assume the voter is perfect both in its ability to produce an output determined by the majority of its inputs and in its ability to identify and to ignore without further delay the outputs of the first faulty element.

The combinatorial method for assessing the reliability of such a structure is entirely straightforward: the probability that the output is correct is simply the probability that at most two of the four elements have failed. If any single element has a probability $P(t)$ of surviving until time t, the probability $R(t)$ that the voter outputs are still correct at time t is therefore

$$R(t) = \sum_{i=0}^{2} \binom{4}{i} [P(t)]^{4-i} [1-P(t)]^{i}$$

$$= 6P^2(t) - 8P^3(t) + 3P^4(t) \qquad (1)$$

The Markov model of the structure in question is equally straightforward. In general, a structure can be represented by a Markov model if it is possible to characterize it in terms of states (the various states defined, for example, by the number of component failures and other relevant parameters) and transition rates between states, with the proviso that the transition rate $r_{ij}(t)$ between state S_i and state S_j is, for all i and j, a function only of i and j and, possibly, the time t measured from the entry into some known initial state (cf. Figure 1). Thus, if the system is known to be in state S_i at time τ, the probability $S_i(t)$ that it has not left that state by time $t \geq \tau$ is given by the solution to the differential equation

$$-S_i'(t) = \sum_j r_{ij}(t) S_i(t) \qquad t \geq \tau$$

with the initial condition $S_i(\tau) = 1$.

If the transition rates $r_{ij}(t)$ are all independent of t, the Markov model is said to be (time) homogeneous. In this case, the differential equation is readily solved, yielding

$$S_i(t) = e^{-\lambda(t-\tau)} \qquad t \geq \tau$$

with $\lambda = \sum_j r_{ij}$. The holding time in each state, in this case, is exponentially distributed.

Consequently, if in the structure of concern here, the probability P(t) that any single element survives until time t is exponentially distributed ($P(t) = e^{-\lambda t}$), and if state S_i refers to

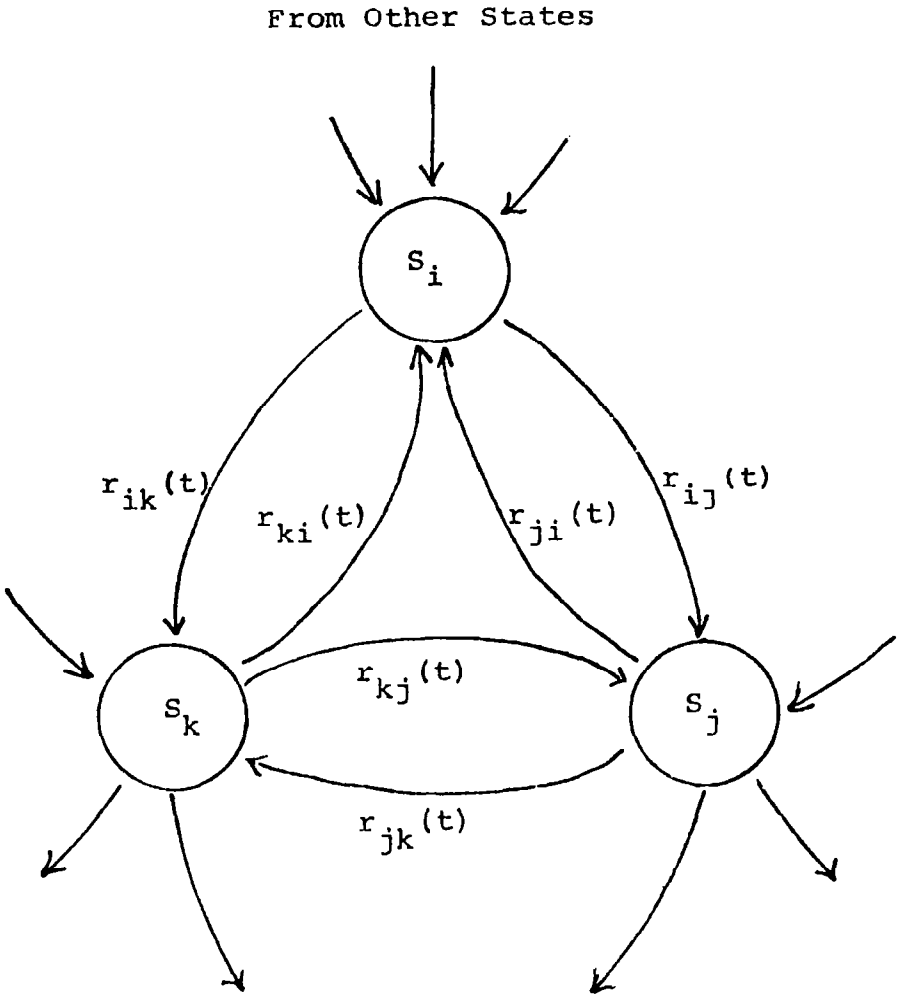


Figure 1

General Structure of a Markov Model

the state of the system characterized by i component failures, then the distribution of the holding time in state i is just $e^{-(4-i)\lambda t}$, with 4 the number of initially operational elements and λ the hazard rate of each element. The transition rate $r_{ij}(t)$ is then simply

$$r_{ij}(t) = \frac{P_i'(t)}{P_i(t)} = \begin{cases} (4-i)\lambda & j = i+1 \\ 0 & j \neq i+1 \end{cases}$$

and the Markov model is as shown in Figure 2. The three states,

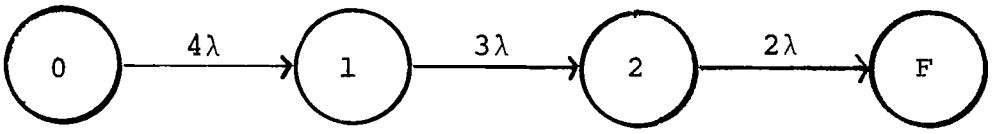


Figure 2

Markov Model of a 2-Out-of-4 Structure

labeled 0, 1, and 2, correspond to the number of failed elements; the state labeled F denotes the failed state (more than two failed elements).

The reliability of the structure is also easy to determine from its Markov model: Let $P_0(t)$ be the probability that the system is in state i at time t. Then

$$\begin{aligned} P_0'(t) &= -4\lambda P_0(t) \\ P_1'(t) &= 4\lambda P_0(t) - 3\lambda P_1(t) \\ P_2'(t) &= 3\lambda P_1(t) - 2\lambda P_2(t) \\ P_F'(t) &= 2\lambda P_2(t) \end{aligned} \qquad (2)$$

This set of linear, first-order differential equations can be solved by conventional methods to yield

$$\begin{aligned} P_0(t) &= e^{-4\lambda t} \\ P_1(t) &= 4e^{-3\lambda t}(1-e^{-\lambda t}) \\ P_2(t) &= 6e^{-2\lambda t}(1-e^{-\lambda t})^2 \\ P_F(t) &= 1-P_0(t) - P_1(t) - P_2(t) \end{aligned} \tag{3}$$

so that

$$R(t) = 1 - P_F(t) = 6e^{-2\lambda t} - 8e^{-3\lambda t} + 3e^{-4\lambda t} \tag{4}$$

as before.

The analysis so far has assumed perfect coverage. In particular, it has been assumed that the first faulty element is correctly identified with probability 1. Suppose, instead, that it is correctly identified with probability C; i.e., with probability 1-C the outputs of the first failed element are not ignored by the voter. Then with probability 1-C, a second failure will cause the voter to accept two erroneous inputs and hence to produce an unreliable output. The system reliability can be determined combinatorially by observing that the system will function properly if at time t it has sustained no more than one element failure or, with probability C, if it has sustained exactly two element failures. Thus,

$$\begin{aligned} R(t) &= \sum_{i=0}^{1} \binom{4}{i} [P(t)]^{4-i}[1-P(t)]^i \\ &\quad + \binom{4}{2} C[P(t)]^2[1-P(t)]^2 \\ &= R^*(t) - 6(1-C)[P(t)]^2[1-P(t)]^2 \end{aligned} \tag{5}$$

with $R^*(t)$ the perfect-coverage reliability as given in equation 1.

The Markov model of Figure 2 needs only to be modified as shown in Figure 3 to account for this imperfect coverage effect. An analysis virtually identical to that of the previous Markov

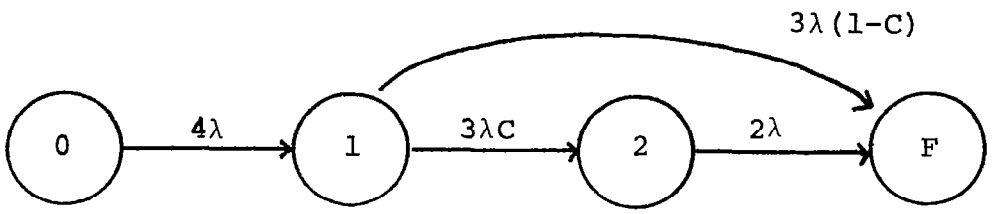


Figure 3

Markov Model of a 2-Out-of-4 Structure With Imperfect Coverage

model establishes that

$$
\begin{aligned}
P_0(t) &= e^{-4\lambda t} \\
P_1(t) &= 4e^{-3\lambda t}(1-e^{-\lambda t}) \\
P_2(t) &= 6Ce^{-2\lambda t}(1-e^{-\lambda t})^2 \\
P_F(t) &= 1-P_0(t) - P_1(t) - P_2(t)
\end{aligned}
\tag{6}
$$

so that, again, the combinatorial model and the Markov model yield identical results.

The procedures for extending both the combinatorial and the Markov methodologies to more complex structures are generally straightforward. One of the major limitations to both approaches, however, is already evident in the simple example just considered. This limitation stems from the fact that it is rarely satisfactory to treat the coverage probability as a constant parameter. And since, as already observed, coverage failures are typically the dominant source of system failure in highly reliable systems, it is particularly important that coverage be accurately modeled.

Suppose, for example, that in the structure just considered, the reason coverage failures can occur is that a certain amount of time, say τ seconds, is needed to detect that an element has failed and to take the appropriate action to eliminate its output from subsequent voter inputs. Should a second failure occur during that interval, the voter is again presented with two potentially erroneous inputs and its output is consequently unreliable. The probability of a coverage failure, then, is the probability that two element failures occur within a τ-second interval. Unfortunately, this is not a constant probability.

To handle this case combinatorially, observe that the probability that the system has failed by time t is equal to the probability that it has sustained either more than two failures, or exactly two failures within τ seconds of each other. Thus,

$$1 - R(t) = \sum_{i=3}^{4} \binom{4}{i} [P(t)]^{4-i} [1 - P(t)]^{i} + 4 \cdot 3 P^{2}(t) \int_{0}^{t} \int_{\eta_1}^{\min[\eta_1+\tau, t]} P'(\eta_1) P'(\eta_2) d\eta_2 d\eta_1 \tag{7}$$

If, as assumed earlier, $P(t) = e^{-\lambda t}$, this expression is easily evaluated, yielding

$$R(t) = \begin{cases} 4P^{3}(t) - 3P^{4}(t) & t < \tau \\ R^{*}(t) - 6P^{2}(t)[(1 - e^{-\lambda\tau}) - P^{2}(t)(e^{\lambda\tau} - 1)] & t \geq \tau \end{cases} \tag{8}$$

with $R^{*}(t)$ as previously defined. The actual coverage probability (cf. equations 5 and 8) in this case is

$$C = C(t) = \begin{cases} 0 & t < \tau \\ 1 - \dfrac{(1 - e^{-\lambda\tau}) - P^{2}(t)(e^{\lambda\tau} - 1)}{[1 - P(t)]^{2}} & t \geq \tau \end{cases} \tag{9}$$

and is indeed a function of time.

The Markov method of modeling redundant structures can also be extended to include more complex coverage situations by using the method of stages (Ref. 1).

The state diagram shown in Figure 4a illustrates the principle.

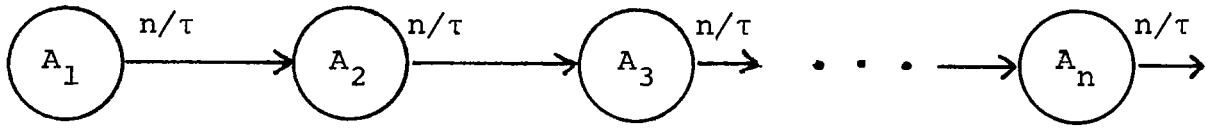


Figure 4a

Stage Representation of a Constant Delay

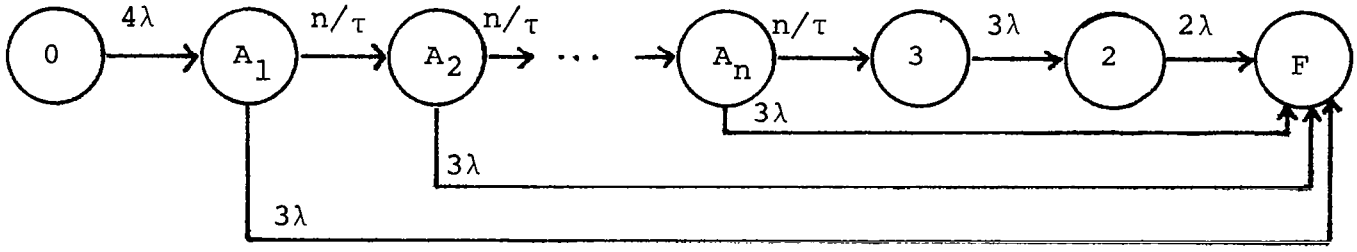


Figure 4b

Markov Model of a 2-Out-of-4 Structure

With Constant Coverage Delay

This diagram is characterized by the differential equation

$$P_{A_1}'(t) = -n/\tau \; P_{A_1}(t)$$

$$P_{A_i}'(t) = n/\tau \; (P_{A_{i-1}}(t) - P_{A_i}(t)) \qquad 1 < i \leq n$$

These are easily solved to yield, when $P_{A_1}(0) = 1$,

$$P_{A_i}(t) = \frac{(nt/\tau)^{i-1}}{(i-1)!} e^{-nt/\tau} \qquad 1 \leq i \leq n$$

Thus, the expected delay E(t) from entry into state A_1 to exit from state A_n is

$$E(t) = \int_0^\infty \sum_{i=1}^{n} P_{A_i}(t)\,dt = \tau$$

and the variance of that delay is

$$Var(t) = 2\int_0^\infty \sum_{i=1}^{n} tP_{A_i}(t)\,dt - E^2(t) = \tau^2/n$$

For large n, then, the series of states shown in Figure 4a provides a good approximation to a constant τ-second delay. This same series of states embedded in the Markov model of a 2-out-of-4 structure (Figure 4b) represents, approximately, the constant coverage delay model under consideration here.

This method of stages can be generalized by introducing other combinations of pseudo-states and selecting appropriate interstage transition rates. The advantage of this technique is that it provides an approximate method for handling non-exponentially distributed holding times without abandoning homogeneous Markov models. The disadvantage is that good approximations often entail a substantial increase in the number of required states, a number which can be enormous for the reliability models of interest here even without the addition of pseudo-states.

It is possible to avoid adding pseudo-states and still retain some advantages of the Markov method by generalizing the notion of a Markov process. Consider the state diagram shown in Figure 5.

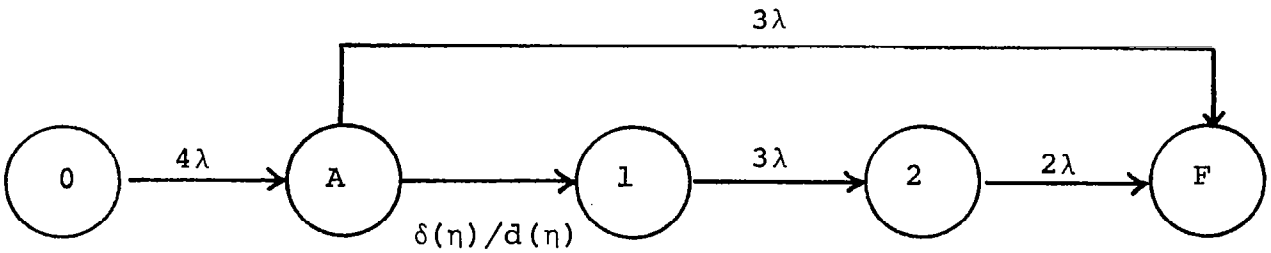


Figure 5

Semi-Markov Model of a 2-Out-of-4 Structure

With Imperfect Coverage

This diagram is similar to that of Figure 4b except that the n pseudo-states in the latter diagram have been collapsed into a single state here. The cost of doing this is to introduce a transition rate* $\delta(\eta)/d(\eta)$ which is now a function of the time η from the entry into state A. If η were a measure of the time from entry into the initial state of the model, the model would describe an inhomogeneous Markov process. As it is, however, the process is not even Markov; the probability of a transition from state A to state 1 is a function not only of the two states but of the time spent in state A as well. Such processes are called semi-Markov (Ref. 2).

Semi-Markov processes, while less analytically tractable than Markov processes, can nevertheless be represented in terms of linear integral equations and the state-occupation probabilities can often be obtained without undue difficulty. The state-occupation probabilities $P_i(t)$ of the process of Figure 5, in particular, satisfy

---

*The function $\delta(\eta)$ here represents the probability density of a transition from state A to state 1 exactly η time units after a transition into state A, under the condition that no other transitions were possible, and $d(\eta)$ is the probability that no such transition has yet taken place by time η. Thus, the rate of such transitions, under the condition just described, is given by the ratio $\delta(\eta)/d(\eta)$.

the following set of equations:

$$
\begin{aligned}
P_0(t) &= e^{-4\lambda t} \\
P_A(t) &= 4\lambda \int_0^t e^{-\lambda(t-\eta)} d(\eta)\, d\eta \; e^{-3\lambda t} \\
P_1(t) &= 4 \int_0^t (1-e^{-\lambda(t-\eta)})\, \delta(\eta)\, d\eta \; e^{-3\lambda t} \\
P_2(t) &= 3\lambda \int_0^t P_1(\eta) e^{-2\lambda(t-\eta)} d\eta
\end{aligned}
\tag{10}
$$

(The probability $P_A(t)$, for example, is just the product of the probability density of a failure at time $t-\eta$, the probability $d(\eta)$ that a transition from state A to state 1 has not taken place in the intervening time η, and the probability $e^{-3\lambda t}$ that no other failure has occurred by time t. Entirely similar arguments can be used to establish the other equations.) In the present example, $\delta(\eta) = \delta_d(\eta-\tau)$ with $\delta_d(t)$ the Dirac delta function and τ the (fixed) coverage delay. Consequently,

$$
d(\eta) = 1 - \int_0^\eta \delta(\eta')\, d\eta' = \begin{cases} 1 & \eta < \tau \\ 0 & \eta \geq \tau \end{cases}
$$

and

$$
\begin{aligned}
P_A(t) &= \begin{cases} 4e^{-3\lambda t}(1-e^{-\lambda t}) & t < \tau \\ 4e^{-3\lambda t}(e^{-\lambda(t-\tau)} - e^{-\lambda t}) & t \geq \tau \end{cases} \\
P_1(t) &= \begin{cases} 0 & t < \tau \\ 4e^{-3\lambda t}(1 - e^{-\lambda(t-\tau)}) & t \geq \tau \end{cases} \\
P_2(t) &= \begin{cases} 0 & t < \tau \\ 6e^{-\lambda(2t+\tau)}(1 - e^{-\lambda(t-\tau)})^2 & t \geq \tau \end{cases}
\end{aligned}
\tag{11}
$$

Since

$$R(t) = P_0(t) + P_A(t) + P_1(t) + P_2(t)$$

this analysis yields results identical to the previous combinatorial analysis of the same example (cf. equations 8 and 11).

As noted earlier, an overwhelming disadvantage of the Markov method of modeling and analyzing the reliability of redundant structures under the conditions of interest here (with the consequent heavy emphasis on coverage) is the extremely large number of states needed to describe the system. This, of course, is only exacerbated if the method of stages is used to approximate non-exponential holding time distributions, but it remains a decisive limitation even if semi-Markov modeling techniques are used.

To gauge the magnitude of the problem, consider a system consisting of n stages.* If the $i^{\underline{th}}$ of these stages can sustain as many as m_i faults and still be operational, and if the number of distinguishable states (e.g., active, benign, detected, etc.) that can be occupied by a stage i fault is ℓ_i, then the number of possible operational system states is

$$N = \prod_{i=1}^{n} \left[\sum_{j=0}^{m_i} \binom{\ell_i+j-1}{j} \right] \qquad (12)$$

This number can be large even for relatively small parameters ℓ_i, m_i, and n. When n=4 and ℓ_i=6, m_i=2 for all i, for example, N = 614,656. Since CARE III actually allows n to be as large as 70 and places no restrictions on m_i, it is clear that conventional Markov-like techniques are not appropriate to the problem at hand.

---

*In CARE III terminology, the term "stage" refers to an ensemble of identical, interchangeable units. This term should not be confused with the "method of stages" described earlier.

Unfortunately, the combinatorial approach to reliability analysis suffers from a similar computational explosion. A combinatorial analysis, in effect, entails an itemization of the (mutually exclusive) sequences of events that can lead to a failure and then a determination of the probability of each of these event sequences. Thus, the emphasis is on the paths connecting the various possible system states rather than on the states themselves. Obviously, however, the number of such paths increases at least as rapidly as the number of states they interconnect, so a purely combinatorial approach to problems of the complexity of those of concern here does not appear to be very attractive either.

3. The CARE III Approach

The motivation for the CARE III approach to reliability analysis is evident from an examination of equation 12. It will be noted, in particular, that the magnitude of N in equation 12 is a very rapidly increasing function of the parameters ℓ_i. (If all ℓ_i were equal to 1 rather than the 6 selected in the earlier example, N would be reduced from 614,656 to 81.) The reason these parameters ℓ_i must, in general, be greater than unity is that the coverage associated with a failure depends upon the states of other failed elements in the system. That is, the probability that the system recovers from a failure in element A may well depend upon whether or not element B has previously failed, whether its failure has been detected, whether an erroneous output has been produced as a result of that failure, and whether element B is in a failed-active state (capable of producing erroneous outputs) or in a failed-benign state (incapable, at least temporarily, of producing further errors).

The key to reducing ℓ_i without decreasing the ability to include all relevant coverage factors into the reliability model is suggested by the previous analysis of the 2-out-of-4 structure. Figure 3 shows a Markov model of that structure with the entire effect of coverage reflected in the state-transition rates. While the coverage probability is shown as a constant in Figure 3, it was demonstrated that the effect of more complex coverage situations could be handled by allowing this probability to be a suitably defined function of time (cf. equation 9).

The CARE III method, then, is to represent the structure of interest as an inhomogeneous Markov model, with the different states distinguished only by the numbers of faults in each of the various stages comprising the system. The state-transition rates are separately determined using a coverage model to account for

fault-state effects. Although combinatorial techniques could have been used (as they were, for example, to derive the results of equation 9), the coverage model found to be most appropriate for CARE III is one based on semi-Markov techniques similar to those used in analyzing the model of Figure 5.

The potential advantage of this approach is apparent. The number of states that have to be accounted for in the reliability model is reduced from that given in equation 12 to a number more manageable:

$$N' = \prod_{i=1}^{n} (m_i+1) \quad \text{(cf. equation 12)}.$$

The cost of doing this, of course, is 1) to force the reliability model to be inhomogeneous*, and 2) to necessitate a separate analysis to determine the needed coverage parameters. For reliability assessment problems of the complexity of concern here, however, the advantages of this approach, in terms of computational effort, far outweigh its disadvantages. In effect, the model has been reduced from one having $N = n_1 \times n_2 \times \ldots \times n_\ell$ states to one having $n_1 + n_2 + \ldots + n_\ell$ states, with n_i denoting the number of relevant states given that i faults have already taken place. (The reduction is in fact more dramatic than this since much of the computational effort needed to determine the transition functions given i faults can also be used to determine these functions given $j \neq i$ faults.)

In order to realize the full advantage of this reliability and coverage model separation, however, it is necessary to introduce

---

*This increased flexibility does have ancillary advantages, however: the hazard rates associated with the various system elements are no longer restricted to be time-independent. There are situations in which this added degree of freedom is needed to reflect accurately the physical events actually being modeled.

some approximations having to do with the probability of occurrence of certain joint events. If A and B represent two events and the probability of an event E is denoted P(E), then, as is well known, the probability that either A or B occurs is

$$P(A+B) = P(A) + P(B) - P(A \cdot B)$$

with $P(A \cdot B)$ the probability that A and B both take place. Now suppose both A and B represent compound events; that is, A is said to have occurred only if the events $A_1, A_2, \ldots, A_n$ have all occurred, and similarly for B. Suppose further, that at least one of the B events, say B_i, is independent of all events in the set $\{A_1, A_2, \ldots, A_n\}$.

Then

$$P(A \cdot B) = P(B|A)P(A) \leq P(B_i)P(A)$$

and

$$P(A)[1-P(B_i)] + P(B) \leq P(A+B) \leq P(A) + P(B)$$

It follows that: 1) P(A+B) is always overbounded by the sum of the probabilities of the two individual events A and B. 2) If either of the two events depends on the occurrence of some subevent that is not part of the other, and if the probability of this subevent is small, the error introduced by approximating P(A+B) by P(A) + P(B) is also small. Specifically,

$$P(A) + P(B) - P(A+B) \leq P(A)P(B_i)$$

In the present instance, the events of concern are those that lead to system failure. The probability of any one of these events is therefore not greater than the probability $P_f(t)$ of system failure, a probability that is already small, for all t of interest, for the highly reliable systems for which CARE III was designed. Thus, if

two events A and B both lead to system failure, if one of these events depends upon a subevent B_i not common to the other, and if the probability of this subevent is also of the order of $P_f(t)$ or less, the error introduced by approximating the probability of either event by the sum of their individual probabilities is of the order of $P_f^2(t)$. Since $P_f(t)$ is almost always less than 10^{-4} for cases of interest here and is typically of the order of 10^{-8} or less (if this were not true, reliability models much simpler than CARE III would suffice), the error introduced by such approximations is truly negligible. Moreover, even if this were not true, such approximations overbound the probability of a system failure and hence provide a conservative reliability estimate in any case. Details as to exactly how these approximations are introduced will become apparent in the ensuing discussion.

(i) The CARE III Reliability Model

Let $P_{j|i}(t|\tau)$ denote the conditional probability that a system is in state j at time t given that it was in state i at time τ. Similarly, let $P_{\ell|j,i}(t|\eta,\tau)$ denote the conditional probability that a system is in state ℓ at time t given that it was in state j at time η and in state i at time τ. Then, clearly, for any $\tau<\eta<t$,

$$P_{\ell|i}(t|\tau) = \sum_j P_{j|i}(\eta|\tau)P_{\ell|j,i}(t|\eta,\tau) \qquad (13)$$

with the sum taken over all the (assumed finite number of) possible intermediate states j. (If, for all $\tau<\eta<t$, $P_{\ell|j,i}(t|\eta,\tau) = P_{\ell|j}(t|\eta)$, then equation 13 reduces to the Chapman-Kolmogorov equation for continuous-time, discrete state systems.)

It follows from equation 13 that

$$P_{\ell|i}(t+\Delta t|\tau) = P_{\ell|i}(t|\tau)P_{\ell|\ell,i}(t+\Delta t|t,\tau) + \sum_{j\neq\ell} P_{j|i}(t|\tau)P_{\ell|j,i}(t+\Delta t|t,\tau) \qquad (14)$$

Let

$$\lambda_{\ell|i}(t|\tau) = \lim_{\Delta t \to 0} \frac{1 - P_{\ell|\ell,i}(t + \Delta t|t,\tau)}{\Delta t}$$

and

$$\lambda_{j\ell|i}(t|\tau) = \lim_{\Delta t \to 0} \frac{P_{\ell|j,i}(t + \Delta t|t,\tau)}{\Delta t}$$

Then, rearranging terms in equation 14, dividing by t and taking the limit as $t \to 0$ yields

$$\frac{\partial P_{\ell|i}(t|\tau)}{\partial t} = -P_{\ell|i}(t|\tau)\lambda_{\ell|i}(t|\tau) + \sum_{j \neq \ell} P_{j|i}(t|\tau)\lambda_{j\ell|i}(t|\tau) \tag{15}$$

This set of equations is a form of the Kolmogorov forward equations. It differs from the more conventional form in that the transition parameters $\lambda_{j\ell|i}(t|\tau)$ are also functions of the initial state i of the system at time τ. If the notation indicating the condition that the system be in state i at time τ is suppressed, equation 15 can be expressed in the more convenient form

$$\frac{dP_{\ell}(t)}{dt} = -P_{\ell}(t)\lambda_{\ell}(t) + \sum_{j \neq \ell} P_{j}(t)\lambda_{j\ell}(t) \tag{16}$$

It must be remembered in the ensuing discussion, however, that the transition parameters may also be functions of the initial conditions.

In the CARE III context, it is necessary to distinguish states both in terms of the number of faults that have been sustained in each stage of the system but also, of course, with regard to

whether or not the system is still operational. The general structure is shown in Figure 6. Here P_ℓ denotes an operational state with ℓ faults and Q_ℓ a failed state with ℓ faults.

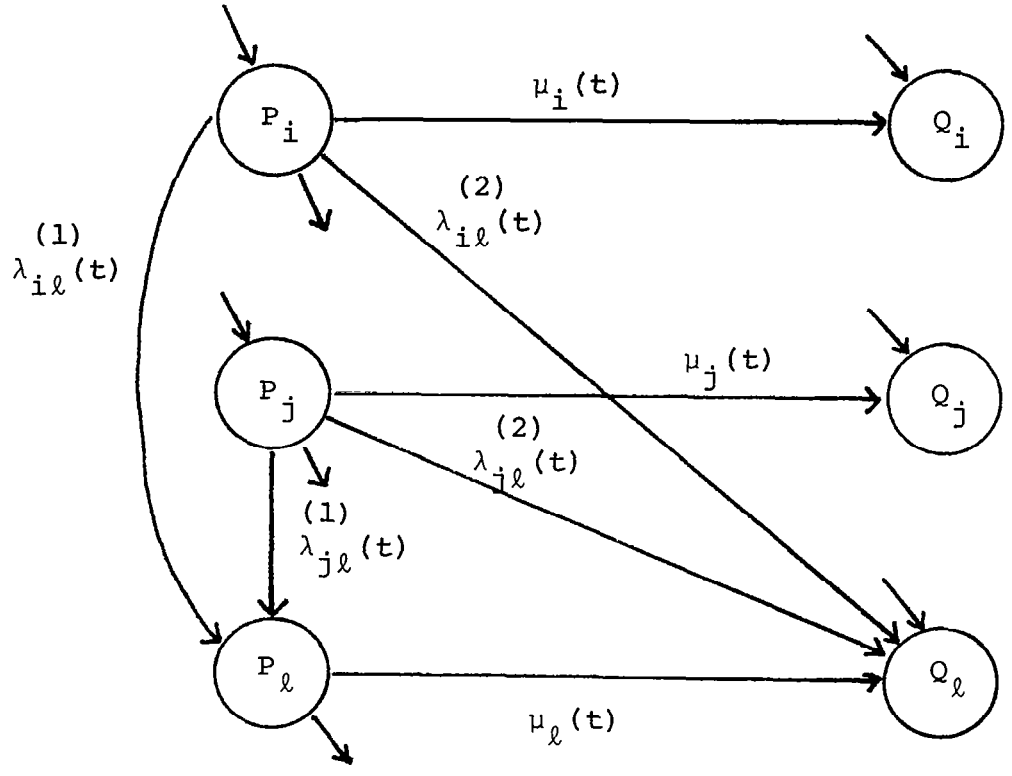


Figure 6

Segment of CARE III Reliability Model

State Diagram

(Since distinction is made as to where the faults are located, the index ℓ is actually an n-component vector with n the number of system stages.) If $P_\ell(t)$ and $Q_\ell(t)$ are the probabilities of being in states P_ℓ and Q_ℓ, respectively, at time t, then Kolmogorov's equations take the form

$$\frac{dP_\ell(t)}{dt} = -P_\ell(t)\lambda_\ell(t) + \sum_{j\neq\ell} P_j(t)\ \lambda^{(1)}_{j\ell}(t) \qquad (17a)$$

$$\frac{dQ_\ell(t)}{dt} = P_\ell(t)\mu_\ell(t) + \sum_{j\neq\ell} P_j(t)\ \lambda^{(2)}_{j\ell}(t) \qquad (17b)$$

with

$$\lambda_\ell(t) = \mu_\ell(t) + \sum_{j\neq\ell} [\lambda^{(1)}_{\ell j}(t) + \lambda^{(2)}_{\ell j}(t)]$$

The term $\mu_\ell(t)$ here represents the rate of occurrence, in a system which is still operational after ℓ failures, of events that cause the system to fail even though no new faults have taken place.* The terms $\lambda^{(1)}_{j\ell}(t)$ and $\lambda^{(2)}_{j\ell}(t)$ represent the rates of occurrence of faults that take the system from operational state j to, respectively, operational state ℓ and failed state ℓ. Since, as has been repeatedly observed in this discussion, the systems of concern here are highly reliable, $\lambda^{(1)}_{j\ell}(t)$ must in general be much larger than $\lambda^{(2)}_{j\ell}(t)$ and $\lambda_\ell(t)$ must be large compared to $\mu_\ell(t)$. Thus, to a good approximation, equation 17a can be rewritten in the form

$$\frac{dP_\ell(t)}{dt} = -P_\ell(t)\lambda_\ell{}^*(t) + \sum_{j\neq\ell} P_j(t)\lambda_{j\ell}{}^*(t) \qquad (18a)$$

with $\lambda_{j\ell}{}^*(t) = \lambda^{(1)}_{j\ell}(t) + \lambda^{(2)}_{j\ell}(t)$ and $\lambda_\ell{}^*(t) = \sum_{j\neq\ell} \lambda^{*}_{\ell j}(t)$. And, if

---

*Such events can be caused, for example, by latent faults becoming active or producing erroneous outputs; this will be elaborated upon shortly.

the solutions to these equations are denoted by $P_\ell^*(t)$, equation 17b assumes the approximate form

$$\frac{dQ_\ell(t)}{dt} = P_\ell^*(t)\mu_\ell(t) + \sum_{j\neq\ell} P_j^*(t)\lambda_{j\ell}^{(2)}(t) \qquad (18b)$$

Although the differential equations (17) could be solved directly, the approximations introduced in replacing $P_\ell(t)$ by $P_\ell^*(t)$ are indeed negligible for all cases of interest. It will be observed, in fact, that $P_\ell^*(t)$ is just the probability that the system would be operating with ℓ failures were the coverage perfect. Thus, replacing $P_\ell(t)$ in equation 17b by $P_\ell^*(t)$ is equivalent to allowing systems that have already suffered from a coverage failure to be counted among those still susceptible to coverage failures. This is, in turn, equivalent to replacing P(A+B) with P(A) + P(B) with A and B both representing highly unlikely coverage failure events. As noted earlier, such approximations introduce an error of the order of p^2 with p the, in this case, very small probability of either of these events by itself. The advantage of introducing this approximation is that the probabilities $P_\ell^*(t)$ can be readily evaluated using straightforward combinatorial techniques, thereby avoiding the need for the more time consuming, and negligibly more accurate, calculation of the probabilities $P_\ell(t)$ as defined by the equation 17a.

(ii) The Coverage Model

The purpose of the CARE III coverage model is to determine the transition rates, $\mu_\ell(t)$ and $\lambda_{j\ell}^{(2)}(t)$, needed to calculate the failed state probabilities $Q_\ell(t)$ as defined by the set of equations 18b. CARE III recognizes three basic causes of coverage failure: 1) An existing latent fault causes the system to take some unacceptable action (an error is propagated). 2) A new fault occurs which,

in combination with an existing latent fault, prevents the system from functioning properly. 3) A pair of existing latent faults for the first time reach a system-disabling state. The transition rates associated with the first and third of these events are collectively represented by the term $\mu_\ell(t)$ in the equations 18b; the rate of occurrence of the second type of event is represented by the term $\lambda_{j\ell}^{(2)}(t)$. A fault is said to be latent from the time it first occurs until it is either detected and isolated from the system or, in the case of a transient fault, reaches a benign state. The function of the coverage model is to represent the behavior of each fault during its latency period.

Note that the second and third causes of coverage failure both depend on the existence of a pair of latent faults. It often happens that a fault, while entirely benign itself, can become lethal in combination with some other fault. (A triple-modular redundant configuration consisting of three identical elements feeding a majority voter is an obvious example of this. If any one element malfunctions, its output is ignored by the voter. If a second element fails before the first failure is detected, however, the combination of the two could well produce an erroneous output.) In many reliability analyses, such second-order effects are negligible compared to other causes of failure and consequently are simply ignored. In the highly reliable systems for which CARE III was designed, however, such effects are frequently the dominent cause of system failure.

Obviously, not all pairs of latent faults pose any threat to the system. Faulty modules providing inputs to two independent voters, for example, should create no difficulty even if both are simultaneously in the active, error-producing, state. It is therefore necessary for the user to specify all <u>critical pairs</u> of

faults; i.e., to specify those pairs of modules which could cause the system to fail should the second modules malfunction before the first one has been identified as faulty. (This critical-pair specification is easily accomplished using the same input routine used to specify the overall system configuration; see below.)

The coverage model thus actually consists of two coverage models: a single-fault model to trace the various states of a single fault, and a double-fault model to track fault pairs. The single-fault model is shown in Figure 7. When a fault first occurs, it is said to be in the active state (state A in Figure 7). If the fault is transient or intermittent, it may jump from the active to the benign state (state B). These transitions take place at a constant rate α; for permanent, non-intermittent faults, of course, $\alpha = 0$. If the fault is intermittent, the reverse, benign-to-active, transition takes place at some constant rate β; for transient faults, $\alpha \neq 0$ and $\beta = 0$. In the benign state, the fault is incapable of causing any discernable malfunction. Thus, it can neither be detected nor can it produce erroneous output. In the active state, however, the fault is both detectable and capable of producing incorrect output. The rate at which either of these events takes place depends upon the operating environment and, in particular, on how frequently and how often the faulty element is exercised in a way that causes the defect to manifest itself. Once an erroneous output is produced, the system is said to be in the active-error state (A_E). Again, if the fault is either intermittent or transient, it may jump to the benign state, although now the error is still present so the state is designated the benign-error state (state B_E; the reason for distinguishing between states A_E and B_E will shortly become apparent). When the faulty element is in either of the two error states, the error propagates at some rate $\epsilon(\tau)$, τ measured from the time of entry into that state, to some point in the system at which it is either

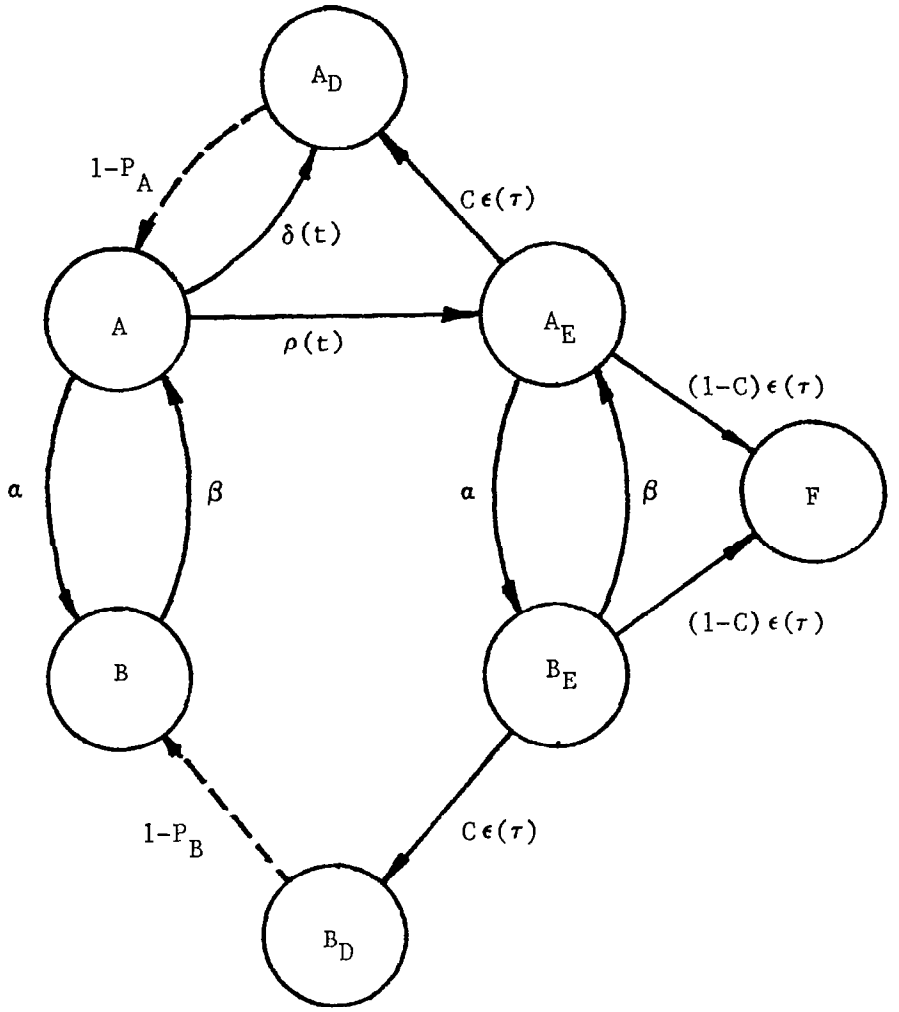


Figure 7

CARE III Single-Fault Model

t = time from entry into active state

τ = time from entry into error state

detected (e.g., through a decoder or a voter) or else escapes undetected and results in a system failure (state F). The probabilities of these two alternatives is C and 1-C, respectively. If the fault is detected, either through testing or through the detection of an erroneous output, the faulty element enters the active-detected state A_D or benign-detected state B_D, depending on the state of the fault when it was detected. At that time a decision is made as to whether the faulty element is to be retired from the system or whether it can continue to be used. This latter decision might be made, for example, if the fault recovery procedure included a diagnostic routine designed to distinguish between permanent and transient faults. If the fault is detected in the active state, the decision is made with probability P_A that the element must be retired from service; if it is detected in the benign state, the same decision is made with probability P_B. Thus, with probabilities $1-P_A$ and $1-P_B$, respectively, the faulty element is returned to service following the detection of the fault. (The dashed lines in Figure 7 indicate that the transition takes place immediately with the probability indicated.)

Note that as long as the option is available to diagnose a detected fault as transient, it is possible that this decision is made erroneously. Thus P_B and even P_A may be less than unity even when the fault is in fact permanent or intermittent. Similarly, P_B and especially P_A may be greater than zero when the fault is indeed transient. The model assumes that the effect of a decision that the fault is transient is to eliminate the error, if an error had already been produced, and to return the faulty element to the error-free, active or benign state, depending on its state when the fault was detected. If the fault was transient and detected in the benign state, it either remains in the benign-detected state or returns to

the error-free benign state. In either case, since $\beta = 0$, it can never again become active so it ceases to pose any further threat to the system. If the fault is transient and detected in the active state, or if it is permanent or intermittent and detected in either state, and if it is diagnosed as transient, it remains latent and may have another chance to cause the system to fail.

Even more detailed single-fault models could, of course, be defined. Non-constant active-to-benign and benign-to-active transition rates could be allowed, for example, and distinctions could be made between single and multiple errors. Moreover, such models could easily be incorporated into the CARE III structure. The model selected, however, was felt to be an effective compromise between the desire to allow the user as much flexibility as possible in defining the behavior of a faulty element, and the need to keep the model from becoming so baroque that the user dispairs of ever defining all of the parameters. At present, the fault detection rate $\delta(t)/d(t)$, the fault generation rate $\rho(t)/r(t)$, and the error propagation rate $\varepsilon(t)/e(t)$ are all restricted to assume the form

$$\phi(t)/[1 - \int_0^t \phi(\eta)\,d\eta]$$

with

$$\phi(t) = \phi e^{-\phi t} \qquad 0 < t$$

or

$$\phi(t) = \begin{cases} \phi & 0 < t < 1/\phi \\ 0 & \text{otherwise} \end{cases}$$

That is, either the transition rates or the transition density functions are assumed to be constant over some range; the function and, of course, the constant can be independently selected by the user for each of the three transition rates. In addition, the user

can define up to five fault types, each with its own set of specifiers (α, β, $\delta(t)$, $\rho(t)$, $\varepsilon(t)$, C, P_A, P_B), and designate that any or all of these types can afflict each of the system stages, with arbitrary rates of occurrence for each type at each stage.

It might be supposed that the double faults could be modeled by simply combining two single-fault models and then determining if, and when, the two independent fault states form some lethal combination. The problem with this approach is that the two fault states may independently form a lethal combination repeatedly and the same system failure thereby counted multiply. (Since a second entry into a state is not necessarily a small-probability event given that the first entrance took place, the previously-used argument, that the probability of both events is of the order of the square of the probability of either of them, is not applicable here.) It is therefore necessary to introduce a separate double-fault model. The model selected is shown in Figure 8. This model is applicable if a second fault occurs when the first fault is in the benign (error-free) state. (If this is not the case, the combination of the two faults is treated as lethal upon the occurrence of the second fault; see below.) Thus, the occurrence of the second fault places the fault-pair in the A_2B_1 state (first fault benign, second fault active). From there, the fault-pair can go to the B_1B_2 state (both faults benign) if the second fault becomes benign before the first fault becomes active, to the detected state D if the active fault is detected and diagnosed as permanent, or to the failed state F if the first fault becomes active with the second fault still also in the active state or if the second fault causes an error to be produced. Since both faults are benign in the B_1B_2 state, the only possible transitions from that state are back to

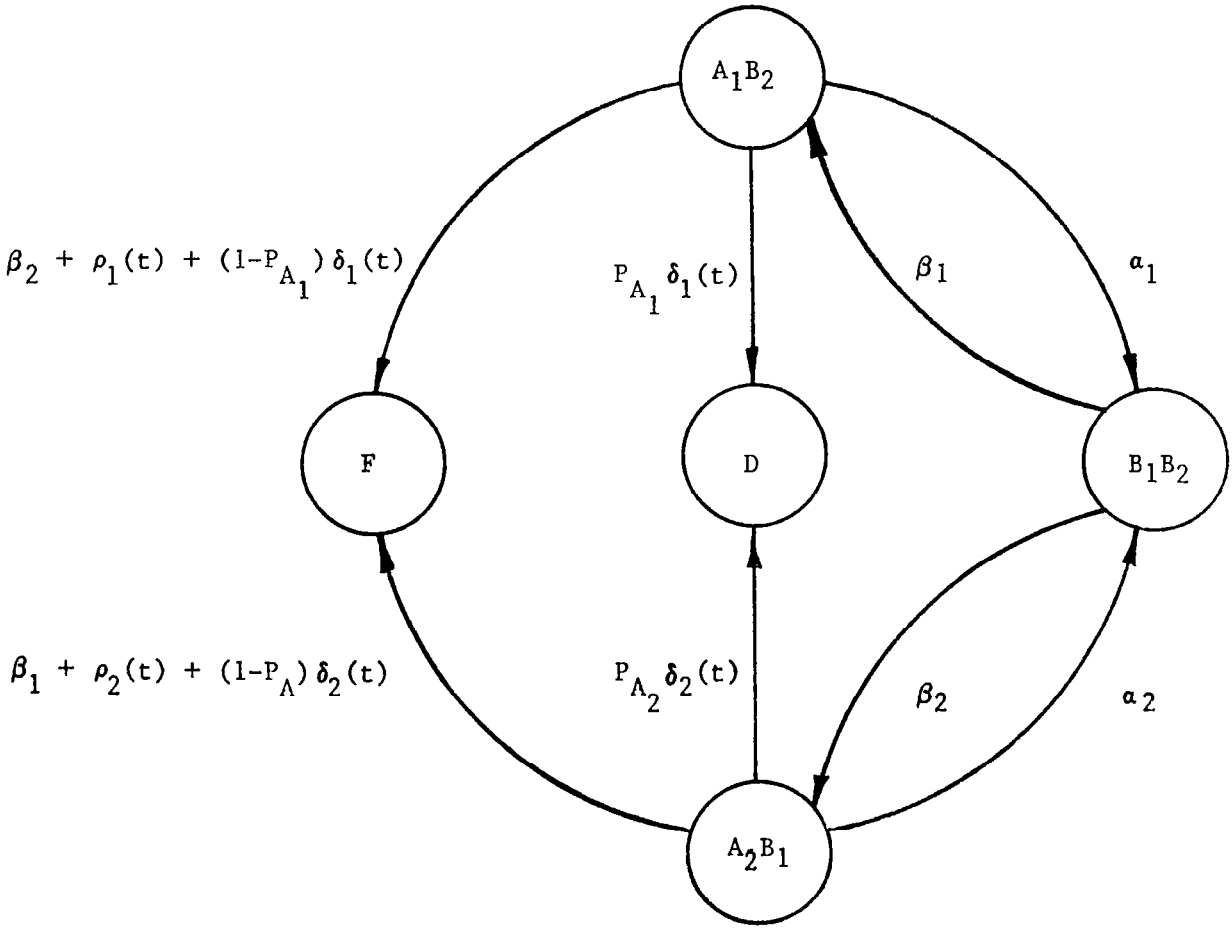


FIGURE 8

CARE III DOUBLE FAULT MODEL

the A_2B_1 state or to the A_1B_2 state (first fault active, second fault benign) with its entirely analogous transitions.

It will be noted that the double-fault model is conservative, relative to the single-fault model, in its definition of a failed state. If both faults are ever simultaneously active, the system fails regardless of whether or not either fault has resulted in an error. Moreover, a system failure results if either fault produces an error even though that error could potentially be detected before it causes any system damage. Obviously, a more elaborate model could have been postulated, one containing additional states to distinguish, among other things, the various possible error conditions. As ih the case of the single-fault model, however, a compromise is required between the need to model accurately the important contributors to coverage failures and the desire not to overburden the user with overly-fine distinctions. If both faults in a critical-pair are active, for example, and one of them produces an error, the probability that that error is detected before it causes system damage is presumably altered, possibly significantly, by the presence of the second fault. Similarly, the coverage parameters may well be affected if both faults produce errors before either error propagates. A more elaborate double-fault model would force the user to examine these issues for every critical-fault pair.

The compromise represented by the double-fault model seems to be a reasonable one for two reasons: 1) The most significant event in determining the probability of a lethal double-fault is the existence of the latent first fault at the time of the second. The probability of this event, however, is determined using the single-fault model and hence does not depend on the details of the double-fault model. 2) .The conservativism of the double-fault model causes the probability of a double-fault coverage failure to be overbounded.

Thus, the double-fault model is consistent with the other CARE III approximations in that it results in a tight overbound on the system unreliability.

The single- and double-fault coverage models are used by the CARE III reliability model as follows: Let $p_f(t-\tau|\ell,t)$ be the probability density of a specific type of element failure at time $t-\tau$, given that ℓ failures have occurred by time t. Then, if $p_{CF}(\tau,f)$ is the probability density of system failures due to the single fault f τ time units after its occurrence, the rate of occurrence of system failures at time t due to this event is just

$$\mu_\ell^{(1)}(t,f) = \int_0^t p_{CF}(\tau,f)\,p_f(t-\tau|\ell,t)\,d\tau \qquad (19)$$

Similarly, if $P_A(\tau,f)$ and $P_B(\tau,f)$ are the probabilities that the fault f is in the active and benign states, respectively, τ time units after its occurrence and if $p_{CF}(\tau,f_1,f_2)$ is the probability density of system failures due to the critical-fault-pair f_1,f_2 τ time units after the occurence of the second fault, the rate of system failures at time t due to the first of a critical pair of faults being active when the second takes place is

$$\lambda_{j\ell}^{(2)}(t,f_1f_2) = p_{f_2}(t)\int_0^t P_A(\tau,f_1)\,p_{f_1}(t-\tau|\ell,t)\,d\tau \qquad (20)$$

with j representing the number of element failures before the fault f_2 and ℓ the number after f_2. (Recall that, in general, j and ℓ are vectors whose components indicate the number of failures in each stage.)

The rate of system failures at time t due to a critical-fault-pair subsequent to the second fault is

$$\mu_{\ell}^{(2)}(t,f_1,f_2) = \int_0^t p_{CF}(\tau|f_1,f_2)p_{f_2}(t-\tau_2|\ell,t)$$

$$\int_0^{t-\tau_2} P_B(\tau_1|f_1)p_{f_1}(t-\tau_1-\tau_2|\ell,t)d\tau_1 d\tau_2 \qquad (21)$$

The transition rates indicated in Figure 6 are thus

$$\mu_{\ell}(t) = \sum_{\text{all } f} \mu_{\ell}^{(1)}(t,f) + \sum_{\substack{\text{all critical} \\ \text{pairs } f_1f_2}} \mu_{\ell}^{(2)}(t,f_1,f_2)$$

$$\lambda_{j\ell}^{(2)}(t) = \sum_{\substack{\text{all critical} \\ \text{pairs } f_1f_2}} \lambda_{j\ell}^{(2)}(t,f_1,f_2) \qquad (22)$$

Note that the function $p_f(t-\tau|\ell,t)$ is conditioned on the event that the system has suffered exactly ℓ element failures by time t. Actually, the function of interest is subject to the additional condition that the system has also not failed by time t since the transitions of concern are those taking the system from an operating state to a failed state. Without this added condition, the function $p_f(t-\tau|t,\ell)$ is easily evaluated; with it, it is obviously considerably more difficult. Ignoring this condition, however, is entirely equivalent to replacing $P_{\ell}(t)$ with $P_{\ell}^*(t)$ as previously discussed and introduces errors of the same order of magnitude. That is, the approximation causes this probability $P_f(t)$ of system failure to be overestimated by an amount of the order of $P_f^2(t)$.

(iii) Mathematical Details

The following paragraphs describe in detail the mathematical model as it is implemented in CARE III. As already mentioned,

the system to be modeled is assumed to consist of some number (up to 70) stages with each stage composed of one or more identical interchangeable elements or modules. The modules in each stage are subject to up to five user-defined categories of faults. A fault is characterized in terms of its rate of occurrence and in terms of its coverage model parameters. Fault occurrence rates are constrained to be of the form $\omega\lambda t^{\omega-1}$ (i.e., fault distributions are constrained to be Weibull) with ω and λ user defined. The user can also specify up to five sets of coverage model parameters (α, β, $\rho(t)$, $\varepsilon(t)$, $\delta(t)$, C, P_A, P_B); each such set defines a fault type. (Thus, for example, it is possible to define a permanent fault type, $\alpha = 0$; a transient type, $\alpha \neq 0$, $\beta = 0$; and an intermittent $\alpha \neq 0$, $\beta \neq 0$; each having its own characteristics with regard to detectability, error-propagation, etc.) Fault category x_i then refers to a fault that can affect any module in stage x; it is characterized by the parameters λ_{x_i}, ω_{x_i}, and j with j a fault-type designator.

In addition, the user must specify the number of modules n_x initially available at each stage, the minimum number m_x needed for that stage to function properly, the various combinations of stage failures that constitute a system failure, and the probabilities $b_{xy}(\nu_x,\nu_y)$ that a specific module in stage x forms a critical pair with a specific module in stage y given that ν_x stage-x modules and ν_y stage-y modules are known to have failed and are therefore no longer being used.*

*These last two tasks are both accomplished with relative ease through a CARE III user interface incorporating a program called FTREE developed by Boeing Aircraft Co. and described in the CARE III User's Manual.

On the basis of this user-supplied information, CARE III then determines the system unreliability using the equation

$$\bar{R}(t) = 1 - R(t) = \sum_{\underline{\ell}\varepsilon L} Q_{\underline{\ell}}(t) + \sum_{\underline{\ell}\varepsilon \bar{L}} P_{\underline{\ell}}^{*}(t) \tag{23}$$

with L the set of module failure combinations that would leave the system operational in the absence of a coverage failure, $\bar{L}$ the complementary set, $P_{\underline{\ell}}^{*}(t)$ the probability that the system would be in state $\underline{\ell}$ at time t in the absence of a coverage failure, and

$$Q_{\underline{\ell}}(t) = \int_0^t \left\{ \sum_{y_j} \left[C_{y_j}(\tau|\underline{\ell}-\varepsilon_y) P_{\underline{\ell}-\varepsilon_y}^{*}(\tau)(n_y-\ell_y+1)\lambda_{y_j}(\tau) \right] + A'(\tau|\underline{\ell}) P_{\underline{\ell}}^{*}(\tau) + a'(\tau|\underline{\ell}) P_{\underline{\ell}}^{*}(\tau) \right\} d\tau \tag{24}$$

This equation is seen to be identical to equation 17b with

$$\mu_{\underline{\ell}}(t) = A'(t|\underline{\ell}) + a'(t|\underline{\ell})$$

$$\lambda_{\underline{j}\underline{\ell}}^{(2)}(t) = \sum_{y_j \varepsilon y} C_{y_j}(\tau|\underline{\ell}-\varepsilon_y)(n_y-\ell_y+1)\lambda_{y_j}(\tau)$$

and $\underline{j} = \underline{\ell}-\varepsilon_y$ with ε_y the unit vector denoting a stage-y module.

It will be recalled from equations 19 and 20 that $\mu_{\underline{\ell}}(t)$ and $\lambda_{\underline{j}\underline{\ell}}^{(2)}(t)$ are defined in terms of functions of the form

$$\int_0^t p_2(\tau) p_1(t-\tau)\, d\tau$$

with $p_1(t)$ a measure of the rate at which a certain class of faults occurs and $p_2(\tau)$ a function of the interval τ between that occurrence and the entry of the fault into a particular coverage-model state. Since, typically, faults occur at rates no greater than

one fault every several thousand hours, and since coverage-state time constants are usually of the order of fractions of seconds and rarely exceed a few minutes in duration, $p_1(t)$ is a much more slowly varying function of time than is $p_2(\tau)$. Thus, to a very good approximation

$$p_1(t-\tau) \approx a(t) + \tau b(t) + \tau^2 c(t) \tag{25}$$

over the range of τ for which $p_1(\tau)$ is not negligibly small, with $a(t)$, $b(t)$, and $c(t)$ suitably defined. This approximation is used in CARE III with $a(t)$, $b(t)$, and $c(t)$ defined to make the approximation exact at the two end points and at the midpoint of the range of interest of τ. The major advantage of introducing this approximation is that, with it,

$$\int_0^t p_2(\tau)p_1(t-\tau)d\tau \approx a(t)m_2{}^0(t) + b(t)m_2{}^1(t) + c(t)m_2{}^2(t) \tag{26}$$

with

$$m_2{}^i(t) = \int_0^t \tau^i p_2(\tau)d\tau$$

Thus, the convolution can be separated into two parts, one part depending only on the reliability-model function $p_1(t)$ and the other involving only the first three moments of the coverage-model function $p_2(\tau)$. Moreover, these moments need be evaluated only at those points of time t relevant to the reliability model. This significantly simplifies the interface between the coverage and reliability models.

With these preliminaries, the reliability model functions used in CARE III are itemized in Table 1 and the coverage model functions in Table 2.

Table 1

Reliability Model Functions

FUNCTION	MATHEMATICAL EXPRESSION		DEFINITION
$R_{x_i}(t)$	$e^{-\Lambda_{x_i}(t)}$	PERMANENT	PROBABILITY THAT A GIVEN STAGE x MODULE HAS NOT EXPERIENCED A CATEGORY-x_i FAULT BY TIME t
	$e^{-H_{DPT}(\tau \mid x_i)d\tau}$	TRANSIENT	
$R_x(t)$	$\prod_i R_{x_i}(t)$		RELIABILITY OF A STAGE x MODULE
$a_{x_i}(t)$	$\frac{H_L(t \mid x_i)}{1-R_x(t)}$	PERMANENT	PROBABILITY THAT A GIVEN STAGE x MODULE HAS A CATEGORY-x_i LATENT PERMANENT (TRANSIENT) FAULT AT TIME t GIVEN THAT IT HAS (NOT) EXPERIENCED A PERMANENT OR LEAKY TRANSIENT FAULT BY TIME t
	$H_L(t \mid x_i)$	TRANSIENT	
$a_x(t)$	$\sum_i a_{x_i}(t)$ (PERMANENT)		PROBABILITY THAT A GIVEN STAGE x MODULE HAS A LATENT (PERMANENT) FAULT AT TIME t GIVEN THAT IT HAS EXPERIENCED SOME PERMANENT FAULT BY TIME t

Table 1 (Continued)

Reliability Model Functions

FUNCTION	MATHEMATICAL EXPRESSION	DEFINITION
$P(\mu_x, t \mid \ell_x)$	$\binom{\ell_x}{\mu_x}(1-a_x(t))^{\ell_x-\mu_x} a_x{}^{\mu_x}(t)$	PROBABILITY THAT A SUBSYSTEM CONTAINS μ_x STAGE x LATENT PERMANENT FAULTS GIVEN THAT IT HAS ℓ_x STAGE x PERMANENT FAULTS
$B_{x_i,y_j}(t \mid \underline{\ell})$	$\sum_{\mu_x,\mu_y} b_{x,y}(\ell_x-\mu_x, \ell_y-\mu_y) P(\mu_x, t \mid \ell_x)$ $P(\mu_y, t \mid \ell_y) C(x_i, y_j) a_{x_i}(t) a_{y_j}(t)$	EXPECTED NUMBER OF x_i, y_j-CRITICAL FAULTS AT TIME t GIVEN $\underline{\ell}$ PERMANENT FAULTS
$C(x_i, y_j)$	$\frac{\mu_x \mu_y}{a_x(t) a_y(t)}$ x_i, y_j = PERMANENT, $x \neq y$	
	$\frac{\mu_x(\mu_x-1)}{a_x^2(t)}$ x_i, y_j = PERMANENT, $x = y$	
	$\frac{\mu_x(n_y-\ell_y)}{a_x(t)}$ x_i = PERMANENT, y_j = TRANSIENT	

Table 1 (Continued)

Reliability Model Functions

FUNCTION	MATHEMATICAL EXPRESSION		DEFINITION
$C(x_i,y_j)$ (CONT.)	$\frac{(n_x-\ell_x)\mu_y}{a_y(t)}$	x_i = TRANSIENT y_j = PERMANENT	
	$(n_x-\ell_x)(\mu_y-\ell_y)$	x_i,y_j = TRANSIENT $x \neq y$	
	$(n_x-\ell_x)(n_x-\ell_x-1)$	x_i,y_j = TRANSIENT $x = y$	
$D_{x_i,y}(t\|\underline{\ell})$	$\sum_{\mu_x,\mu_y} b_{x,y}(\ell_x-\mu_x,\ell_y-\mu_y)P(\mu_x,t\|\ell_x)$ $P(\mu_y,t\|\ell_y)$		EXPECTED NUMBER OF x_iy-CRITICAL FAULTS, GIVEN $\underline{\ell}$ PERMANENT FAULTS, THAT WOULD BE CREATED AS THE RESULT OF A STAGE y FAULT AT TIME t
	$\mu_x \frac{a_{x_i}(t)}{a_x(t)}$	x_i = PERMANENT	
	$(n_x-\ell_x)a_{x_i}(t)$	x_i = TRANSIENT	
$C_{y_j}(t\|\underline{\ell})$	$\sum_{x_i} \frac{H_{\bar{B}}(t\|x_i)}{H_L(t\|x_i)} D_{x_i,y_j}(t\|\underline{\ell})$		PROBABILITY THAT A CATEGORY y_j FAULT WOULD PRODUCE A SYSTEM FAILURE AT TIME t GIVEN $\underline{\ell}$ FAULTS AT TIME t^-

Table 1 (Continued)

Reliability Model Functions

FUNCTION	MATHEMATICAL EXPRESSION	DEFINITION
$A'(t\|\underline{\ell})$	$\sum_{x_i,y_j} \frac{h_{DF}(t\|x_i,y_j)}{H_L(t\|x_i)H_L(t\|y_j)} B_{x_i,y_j}(t\|\underline{\ell})$	RATE WHICH SYSTEMS HAVING $\underline{\ell}$ FAULTS FAIL AT TIME t DUE TO CRITICAL FAULT CONDITIONS
$a'(t\|\underline{\ell})$	$\sum_{x_i} \frac{\ell_x h_F(t\|x_i)}{1-R_x(t)}$ PERMANENT $+ \sum_{x_i} (n_x-\ell_x) h_F(t\|x_i)$ TRANSIENT	RATE AT WHICH SYSTEMS HAVING $\underline{\ell}$ FAULTS FAIL AT TIME t DUE TO ERROR PROPAGATION
$H_L(t\|x_i)$	$a_L(t\|x_i)M_L^0(t\|x_i)+b_L(t\|x_i)M_L^1(t\|x_i) + c_L(t\|x_i)M_L^2(t\|x_i)$	PROBABILITY OF A LATENT CATEGORY x_i FAULT AT TIME t
$H_{\overline{B}}(t\|x_i)$	$a_{\overline{B}}(t\|x_i)M_{\overline{B}}^0(t\|x_i)+b_{\overline{B}}(t\|x_i)M_{\overline{B}}^1(t\|x_i) + c_{\overline{B}}(t\|x_i)M_{\overline{B}}^2(t\|x_i)$	PROBABILITY OF A NON-BENIGN LATENT FAULT AT TIME t

Table 1 (Continued)

Reliability Model Functions

FUNCTION	MATHEMATICAL EXPRESSION	DEFINITION
$H_B(t\|x_i)$	$a_B(t\|x_i)M_B^0(t\|x_i)+b_B(t\|x_i)M_B^1(t\|x_i) + c_B(t\|x_i)M_B^2(t\|x_i)$	PROBABILITY OF A BENIGN LATENT FAULT AT TIME t
$H_{DPT}(t\|x_i)$	$a_{DP}(t\|x_i)m_{DP}^0(t\|x_i)+b_{DP}(t\|x_i)m_{DP}^1(t\|x_i) + c_{DP}(t\|x_i)m_{DP}^2(t\|x_i)$	PROBABILITY THAT A CATEGORY x_i TRANSIENT FAULT IS DETECTED AS PERMANENT
$h_{DF}(t\|x_i,y_j)$	$a_{DF}(t\|x_i,y_j)m_{DF}^0(t\|x_i,y_j) + b_{DF}(t\|x_i,y_j)m_{DF}^1(t\|x_i,y_j) + c_{DF}(t\|x_i,y_j)m_{DF}^2(t\|x_i,y_j)$	RATE AT WHICH AN x_iy_j-CRITICAL FAULT CAUSES SYSTEM FAILURE
$h_F(t\|x_i)$	$a_F(t\|x_i)m_F^0(t\|x_i)+b_F(t\|x_i)m_F^1(t\|x_i) + c_F(t\|x_i)m_F^2(t\|x_i)$	RATE OF ERROR PROPAGATION FAILURE DUE TO A CATEGORY x_i FAULT

Table 1 (Continued)

Reliability Model Functions

FUNCTION	MATHEMATICAL EXPRESSION	DEFINITION
$a_X(t\|x_i)$ $a_X(t\|x_i, y_j)$	$f(t) = \begin{cases} \lambda_{x_i}(t) & X = DP,L,B,\bar{B},F \\ & x_i = \text{TRANSIENT} \\ \lambda_{x_i}(t)\,R_x(t) & X = L,B,\bar{B},F \\ & x_i = \text{NON-TRANSIENT} \\ H_B(t\|x_i)\,\lambda_{y_j}(t) & X = DF \\ & y_j = \text{TRANSIENT} \\ H_B(t\|x_i)\,\lambda_{y_j}(t)\,r_y(t) & X = DF \\ & y_j = \text{NON-TRANSIENT} \end{cases}$	WEIGHT FUNCTIONS USED IN CONVOLUTIONAL APPROXIMATION (CF. EQUATION 25)
$b_X(t\|x_i)$ $b_X(t\|x_i, y_j)$ all X	$\begin{cases} -\dfrac{f(t) - f(0)}{t} & t = \Delta t_r \\ -\dfrac{(3k^2-1)f(t) - 2k^2\left[f\left(\frac{t+\Delta t_r}{2}\right) + f\left(\frac{t-\Delta t_r}{2}\right)\right] + (k^2+1)f(0)}{(k^2-1)t} & t = k\Delta t_r, < t_n, \text{ k odd} \\ -\dfrac{3f(t) - 4f(t/2) + f(0)}{t} & t = k\Delta t_r, < t_n, \text{ k even} \\ -\dfrac{3f(t) - 4f(t-t_n/2) + f(t-t_n)}{t_n} & t \geq t_n \end{cases}$	

Table 1 (Continued)

Reliability Model Functions

FUNCTION	MATHEMATICAL EXPRESSION	DEFINITION
$c_X(t\|x_i)$, $c_X(t\|x_i,y_j)$	0	$t = \Delta t_r$
	$\dfrac{f(t) - f\left(\frac{t+\Delta t_r}{2}\right) + f\left(\frac{t-\Delta t_r}{2}\right) + f(0)}{[t^2 - (\Delta t_r)^2]/2}$	$t = k\Delta t_r < t_n$, k odd
	$\dfrac{f(t) - 2f(t/2) + f(0)}{t^2/2}$	$t = k\Delta t_r < t_n$, k even
	$\dfrac{f(t) - 2f(t-t_n/2) + f(t-t_n)}{t_n^2/2}$	$t \geq t_n$
t_n		min $t = n\,t_r$, n even, such that $P_X(t) \leq \theta$ or $P_X(t) \leq \theta$ with θ a user-defined threshold

Table 2a

Single-Fault Model Equations

FUNCTION	MATHEMATICAL EXPRESSION*	DEFINITION
$\phi(t)$	$\alpha e^{-\beta t} \int_0^t e^{-(\alpha-\beta)\tau} r(\tau)\, d(\tau)\, d\tau$	β^{-1} TIMES THE PROBABILITY INTENSITY OF RE-ENTERING STATE A EXACTLY t TIME UNITS AFTER THE PREVIOUS ENTRY
$P_a(t)$	$e^{-\alpha t} r(t)\, d(t) + \beta \int_0^t \phi(t-\tau) P_a(\tau)\, d\tau$	PROBABILITY OF BEING IN STATE A AT TIME t WHEN $P_A = P_B = 1$
$P_b(t)$	$\phi(t) + \beta \int_0^t \phi(t-\tau) P_b(\tau)\, d\tau$	PROBABILITY OF BEING IN STATE B AT TIME t WHEN $P_A = P_B = 1$
$P_e(t)$	$\int_0^t e^{-\alpha\tau} \rho(\tau)\, d(\tau)\, e(t-\tau)\, d\tau + \beta \int_0^t \phi(t-\tau) P_e(\tau)\, d\tau$	PROBABILITY OF BEING IN STATE A_E OR B_E AT TIME t WHEN $P_A = P_B = 1$

* t HERE IS A MEASURE OF THE TIME SINCE THE ENTRY INTO STATE A.

Table 2a (Continued)

Single-Fault Model Equations

FUNCTION	MATHEMATICAL EXPRESSION*	DEFINITION
$p_e(t)$	$e^{-\alpha t}\rho(t)d(t) + \beta\int_0^t \phi(t-\tau)p_e(\tau)d\tau$	INTENSITY OF ENTRY INTO STATE A_E AT TIME t WHEN $P_A = P_B = 1$
$p_{\bar{e}}(t)$	$e^{-\alpha t}\delta(t)r(t) + \beta\int_0^t \phi(t-\tau)p_{\bar{e}}(\tau)d\tau$	INTENSITY OF ENTRY INTO STATE A_D FROM STATE A AT TIME t WHEN $P_A = P_B = 1$
$p_f(t)$	$(1-C)\int_0^t p_e(\tau)\varepsilon(t-\tau)d\tau$	INTENSITY OF ENTRY INTO STATE F AT TIME t WHEN $P_A = P_B = 1$
$\Psi_A(t)$	$C\int_0^t p_e(\tau)\varepsilon(t-\tau)\left(\frac{\beta + \alpha e^{-(\alpha+\beta)(t-\tau)}}{\alpha+\beta}\right)d\tau + p_{\bar{e}}(t)$	INTENSITY OF ENTRY INTO STATE A_D AT TIME t FOR THE FIRST TIME

* t HERE IS A MEASURE OF THE TIME SINCE THE ENTRY INTO STATE A.

Table 2a (Continued)

Single-Fault Model Equations

FUNCTION	MATHEMATICAL EXPRESSION*	DEFINITION
$\Psi_B(t)$	$\frac{\alpha C}{\alpha+\beta}\int_0^t p_e(\tau)\left(1 - e^{-(\alpha+\beta)(t-\tau)}\right)\varepsilon(t-\tau)d\tau$	INTENSITY OF ENTRY INTO STATE B_0 AT TIME t FOR THE FIRST TIME
$\chi_B(t)$	$\int_0^t \Psi_B(\tau)e^{-\beta(t-\tau)}d\tau$	PROBABILITY OF HAVING ENTERED STATE B_D FOR THE FIRST TIME AND THEN REMAINING IN THE BENIGN STATE UNTIL TIME t
$P_{dp}(t)$	$P_A\int_0^t \Psi_A(\tau)d\tau + P_B\int_0^t \Psi_B(\tau)d\tau$	PROBABILITY THAT A FAULT HAS BEEN DIAGNOSED AS PERMANENT BY TIME t
$F_X(t)$	$F_x(t) + \int_0^t [(1-P_A)\Psi_A(t-\tau) + (1-P_B)\beta\chi_B(t-\tau)]F_X(\tau)d\tau$	FUNCTION RELATING PROBABILITIES AND INTENSITIES DERIVED WHEN $P_A = P_B = 1$ TO THOSE SAME QUANTITIES WHEN P_A & P_B ARE ARBITRARY

* t HERE IS A MEASURE OF THE TIME SINCE THE ENTRY INTO STATE A.

Table 2a (Continued)

Single-Fault Model Equations

FUNCTION	MATHEMATICAL EXPRESSION*	DEFINITION
$P_B(t)$	$F_X(t)$ with $F_x(t) = P_b(t) + X_B(t)$	PROBABILITY OF BEING IN STATE B AT TIME t
$P_{\bar{B}}(t)$	$F_X(t)$ with $F_x(t) = P_a(t) + P_e(t)$	PROBABILITY OF BEING IN A NON-BENIGN STATE AT TIME t
$P_L(t)$	$F_X(t)$ with $F_x(t) =$ $P_b(t) + X_B(t)$ + $P_a(t) + P_e(t)$ PERMANENT FAULTS; $P_a(t) + P_e(t)$ TRANSIENT FAULTS	PROBABILITY OF A LATENT FAULT OR UNDETECTED ERROR AT TIME t
$P_{DP}(t)$	$F_X(t)$ with $F_x(t) = P_{dp}(t)$	PROBABILITY THAT A FAULT HAS BEEN DIAGNOSED AS PERMANENT BY TIME t

* t HERE IS A MEASURE OF THE TIME SINCE THE ENTRY INTO STATE A.

Table 2b

Double-Fault Model Equations

FUNCTION	MATHEMATICAL EXPRESSION	DEFINITION
$c_i(t)$	$\beta_i(t)d_j(t)r_j(t)a_j(t) +$	TRANSITION RATE FROM STATE A_jB_i TO STATE F
$i = 1,2$	$(1-P_{A_j})b_i(t)\,\delta_j(t)r_j(t)a_j(t) +$	
$j = 3-i$	$b_i(t)d_j(t)\rho_j(t)a_j(t)$	
$f_i(t)$	$\alpha_j(t)b_i(t)d_i(t)r_i(t)$	TRANSITION RATE FROM STATE A_jB_i TO STATE B_1B_2
$i = 1,2$		
$j = 3-i$		
$c_4(t)$	$\int_0^t [c_1(t-\tau)\beta_2(\tau)b_1(\tau) +$ $c_2(t-\tau)\beta_1(\tau)b_2(\tau)]d\tau$	INTENSITY OF ENTRY INTO STATE F t TIMEUNITS AFTER ENTRY INTO STATE B_1B_2
$c_3(t)$	$\int_0^t [f_1(t-\tau)\beta_2(\tau)b_1(\tau) +$ $f_2(t-\tau)\beta_1(\tau)b_2(\tau)]d\tau$	INTENSITY OF RE-ENTRY INTO STATE B_1B_2 t TIME UNITS AFTER A PREVIOUS ENTRY

Table 2b (Continued)

Double-Fault Model Equations

FUNCTION	MATHEMATICAL EXPRESSION	DEFINITION
$p_3(t)$	$f_1(t) + \int_0^t c_3(t-\tau)p_3(\tau)d\tau$	INTENSITY OF ENTRY INTO STATE B_1B_2 t TIME UNITS AFTER ENTRY INTO STATE A_2B_1
$p_{DF}(t)$	$c_1(t) + \int_0^t c_4(t-\tau)p_3(\tau)d\tau$	INTENSITY OF ENTRY INTO STATE F t TIME UNITS AFTER ENTRY INTO STATE A_2B_1

4. Concluding Remarks

It is, of course, obvious that the more reliable a system becomes, the more improbable are the events that cause it to fail. Accordingly, reliability models designed to estimate the reliability of such systems must necessarily take into account effects which could be ignored or only roughly approximated in models designed for less reliable structures. These effects are generally referred to as coverage effects; that is, effects that result in system failure due, not to an exhaustion of resources, but rather to faults that, while circumventable, are not detected and isolated before they have caused the system as a whole to malfunction.

CARE III is designed to allow the user to model coverage effects to a detail heretofore impossible. To take full advantage of this capability, the user must attempt to specify more completely just how the effects of a fault make themselves manifest to the system. In order to estimate the distribution of the time from the occurrence of a fault to its detection, in particular, consideration must be given to the frequency and thoroughness with which the faulty module is tested. If the module is tested every τ seconds, for example, and if the probability is unity that the fault is detected if it is present when the test is conducted, then the distribution of the time to detection is well modeled as $d(t) = 1-t/\tau$, $0 \leq t \leq \tau$. If, on the other hand, the module is tested at random intervals with a less than certain outcome even if the fault is present, a distribution of the form $d(t) = e^{-\delta t}$ might be more appropriate. Similar considerations are needed to select the other relevant functions and parameters used in the CARE III coverage model.

In many cases, coverage model parameters may be difficult to determine. Even in these cases, it is felt that CARE III can still

play a valuable role for two reasons: 1) It forces the user to examine aspects of the system that might otherwise have been ignored. 2) More importantly, it provides a means for determining the sensitivity of the system's reliability to assumptions made both about the behavior of faults and about the mechanisms provided to recover from them.

Preliminary tests have shown that CARE III is indeed capable of accurately estimating the reliability of a variety of systems under a variety of conditions and assumptions (cf. Ref. 3). These tests are being continued, both at Raytheon and elsewhere, and will be reported on in greater detail later.

REFERENCES

1. Cox, D. R., and H. D. Miller, The Theory of Stochastic Processes, Methuen and Co. Ltd., London, 1968.

2. Feller, William, "On Semi-Markov Processes," Proceedings of the National Academy of Sciences, Vol. 51, pp. 653-659, 1964.

3. Stiffler, J. J., L. A. Bryant, and L. Guccione, CARE III Final Report, Phase I, NASA CR-159122, November 1979.